PCT/AU2004/000338

Australian Government

Patent Office
Canberra

I, JULIE BILLINGSLEY, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2003901468 for a patent by ENTROPIC TECHNOLOGIES PTY LTD as filed on 01 April 2003.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Eighth day of April 2004

J. Billingsley

JULIE BILLINGSLEY
TEAM LEADER EXAMINATION
SUPPORT AND SALES

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

APPLICANT: ENTROPIC TECHNOLOGIES PTY LTD

NUMBER:

FILED:

AUSTRALIA

THE PATENTS ACT 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED

"SYSTEM FOR SECURE COMMUNICATION"

The present invention will be described in the following statement:

TITLE

"SYSTEM FOR SECURE COMMUNICATION"

The present invention relates to a system for securely transmitting information across a communication network, such as the Internet.

Despite the growing number of people and organisations conducting commercial transactions over the Internet, there are still significant concerns regarding the security of such transactions that limit the potential growth of e-commerce on the Internet. While measures are available to provide various levels of security to data transmitted over the Internet, these measures generally have drawbacks in terms of the costs, ease of use and the use of computer resources to provide high levels of security.

The current standard for secure network transmission is Secure Socket Layers (SSL) which uses Public Key Cryptography. Public key cryptography involves the use of a pair of keys, being a public key and a private key. Any data encrypted by one key requires the other key for decryption. This type of encryption is referred to as asymmetric encryption. In symmetric encryption, the same key is used for both encryption and decryption. Asymmetric encryption has the advantage that the sender and receiver of data do not need to have shared the encryption key prior to the communication. The owner publishes the details of the public key and keeps the details the private key secure. Others can send information encrypted with the public key to the owner knowing that only the owner can decrypt it as they alone have the private key. Also the owner can encrypt information with the private key and send this to others. If this information can be decrypted by the public key then the person who decrypts knows it came from the owner of the private key.

It is known however, that for a required encryption strength, keys of greater length are required when using asymmetric encryption in comparison to symmetric key encryption. The longer keys mean more computation and asymmetric encryption is therefore often used to simply send a known key which is then used for symmetric encryption of the data.

With regard to faceless electronic communications there are generally 4 security issues that need to be addressed. These issues are :

Authentication - A means to confirm that the user is who he says he is.

Privacy - A means to ensure that the communication is private and difficult to eavesdrop upon.

Integrity - A means to ensure that the communicated data cannot be tampered with or corrupted.

Non-repudiation - A means to ensure confirmation or authorisation of the transaction so that the user can not deny responsibility for the transaction at a later date.

Most security systems only deal with two of these issues, namely Authentication and Privacy. The last two issues are more difficult to overcome, with the latter being the most difficult. In order to deal with all four of these issues, it will generally be required to integrate various technologies which deal with specific issues, which is expensive and therefore not available to all users.

The present invention provides a system for communicating securely over a communication network, such as the Internet, which attempts to address the above mentioned issues effectively and economically.

In accordance with one aspect of the present invention there is provided a system for secure communication across a communication network comprising:

a personal code generation means having one or more identification codes and one or more encryption codes, the identification and encryption codes being arranged to change at predetermined time intervals; and

a code server synchronised with the personal code generation means such that the code server has information regarding the or each current identification code and the or each current encryption code of the personal code generation means;

wherein a user transmits across the communication network, the or each current identification code of the personal code generation means and data encrypted with the or each current encryption code of the personal code generation means and the code server provides the information regarding the or each current identification code to authenticate the user and the information about the or each current encryption code to decrypt the transmitted data.

The present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a representation of personal tokens for use with a system for secure communication in accordance with the present invention;

Figure 2 is a representation of personal token and corresponding code server for use with the system for secure communication;

Figure 3 is a representation of a system for secure communication in accordance with the present invention implemented on a communication network;

Figure 4 is a representation of an alternative embodiment of a system for secure communication in accordance with the present invention implemented on a communication network; and

Figure 5 is a representation of personal tokens having a plurality of encryption codes for use with the system for secure communication.

Referring to the Figures, there is shown a system for secure communication 10 across a communication network 14. The communication network 14 may be a publicly accessible network, such as the Internet, or a private network.

The system for secure communication 10 includes a code generation means in the form of a personal token 12. The personal token 12 is provided in a physical form such that it is easily carried by a user. The personal token 12 may, for example, be in the form of a pendant 17 or card 18.

The personal token 12 is arranged to generate and/or store information including one or more identification codes 20 that are valid at any point in time and one or more encryption codes 22 that are valid at any point in time. In the embodiment shown in the drawings, the personal token 12 generates and/or stores one current identification code 20 and one current encryption code 22. The personal token may include one or more display means 24 on which the current identification code 20 and the current encryption code 22 can be displayed.

The personal token 12 is provided with a suitable processing means which is capable of changing the identification code 20 and the encryption code 22 at predetermined time intervals.

The secure communication system 10 is also provided with one or more code servers 16 to service a plurality of personal tokens 12. The code server 16 is in the form of a suitable computer connected to the communication network 14. The code server 16 is arranged to generate and/or store information about each of the personal tokens 12 that are serviced by the code server 16, including the identification code 20 and

encryption code 22. The code server 16 is arranged to be synchronised with each of the personal tokens 12 before use of the personal token 12 is commenced by the user. Following synchronisation, the code server 16 will have information about the personal token 12 such that the code server 16 is able to determine the current identification code 20 and encryption code 22 of the personal token 12 at any instant in time.

The user of the personal token 12 is also provided with a Username and/or Password associated with the personal token 12. Either a username or password or both may be provided associated with the personal token 12 but in the embodiment described, both are provided. As the identification code 20 and encryption code 22 are available to the holder of the personal token 12, loss of the personal token 12 by the user could result in a breach of security. Information regarding the username and password for the personal token 12 is stored by credit card server 28 but is not stored by the personal token 12. In this way, unauthorised use of the personal token 12 is restricted. The functions of the credit card company server 28 and the code server 16 may be integrated into a single server if required (not shown).

Figure 3 shows an example of the system for secure communication 10 in use on a communication network 14. In this example, a user operating a user terminal 24 requires to communicate securely with a merchant's server 26 in order to make a purchase. The merchant's server 26 requires to communicate securely with a credit card company server 28 in order to determine if credit card details provided by the user are valid for the purposes of the present purchase. In the embodiment shown in Figure 3, the credit card company has a code server 16 connected securely, for example by a private connection, to the credit card company server 28.

Each of the user terminal 24, the merchant server 26 and the Credit Card company server 28 is provided with encryption software capable of encrypting data to be transmitted over the communication network 14 using an encryption code as the key. In use, when the user wishes to transmit his credit card details to the merchant's server 26, he enters the credit card details into the user terminal 24 along with his username and password. The credit card details are then encrypted by the encryption software using the current encryption code 22 of the personal token 12 which is provided to the encryption software by the user. The encrypted information is then transmitted along with the username and password and the current identification code 20 displayed on the personal token 12 to the merchant's server 26 over the communication network 14. The current encryption code 22 is not transmitted across the communication network 14.

While in the present embodiment, the information generated and/or stored on the personal token 12 is displayed for viewing and then entered manually into the user terminal 24, the personal token 12 may be provided with a communication port (not shown) arranged to connect directly to the user terminal and provide the identification code 20 and encryption code 22 to the user terminal via the communication port. The merchant's server 26 receives the username and password, the current identification code 20 and the encrypted information from the user terminal 24 and re-transmits to the credit card company server 28 for validation of the username and password against the current identification code 20 and against the credit card details. The credit card company server 28, against the username and password received, requests from the code server 16 its corresponding identification code and verifies that it matches the current identification code 20 received. Following this

authentication verification, the credit card company server 28 requests from the code server 16 its corresponding decryption code, which should be the same as the encryption code 22 for the time the information was encrypted and therefore be able to decrypt the information. The decrypted information, decrypted in the credit card company server 28 is compared against the valid credit card details and the merchant's server 26 is advised, via the communication network 14, whether the transaction may proceed. In the event that any of the steps of verification fail, the user will be notified via the communication network 14 that the transaction cannot proceed and may be requested to enter all the required details again.

While this example shows only transmission of information from the user to the location of the credit card company server 28 and its code server 16, information being transmitted in the opposite direction could be transmitted using the same means. That is, if information needs to be transmitted across the communication network 14 to the user from the credit card company, the identity of the credit card company is authenticated with the current identification code 20 provided by the code server 16 and the information would be encrypted with the current encryption code 22 provided by the code server 16. The user could then decrypt the information by providing the encryption code 22 from the personal token 12 to the encryption software on the user terminal 24.

Figure 4 shows an alternative arrangement of the system for secure communication 10 shown in Figure 3. In Figure 4, the Credit card company does not have their own code server 16. The code server 16 is provided at another location and may communicate with the credit card company server 28 via a code network server 30 also connected to the communication network 14. It is foreseeable that some organisations may not be

able to justify the expense of their own code server 16 and use an arrangement such as this. The method for communication in this case is the same as previously described with the exception of the communication between the credit card server 28 and the code server 16. In this case, as the information is not being passed over a private connection, the information passing between the credit card company server 28 and the code server 16 must also be encrypted. The credit card company in this case will possess their own personal token 12 or another form of code generation means which can be used in the same manner as described above to encrypt transmissions between the credit card company and the code server 16.

The system for secure communication 10 described will allow any two computers provided with personal tokens 12 or another form of code generation means within a network to communicate securely, in effect providing in effect multiple 'virtual private channels' within any network or communication means irrespective of the network protocol or communication means.

Figure 5 shows alternative embodiments of personal tokens 12 in which a plurality of encryption codes 22 are provided on the personal token 12. In the embodiment shown, two encryption codes 22 are used. The personal token 12 of Figure 5 may be used in a system for secure communication wherein the method of encryption of data utilises both encryption codes 22 for greater security.

Modifications and variations as would be apparent to a skilled addressee are deemed to be within the scope of the present invention.

DATED THIS 31st DAY OF MARCH 2003.

ENTROPIC TECHNOLOGIES PTY LTD
By their Patent Attorneys
LORD & COMPANY
PERTH, WESTERN AUSTRALIA.

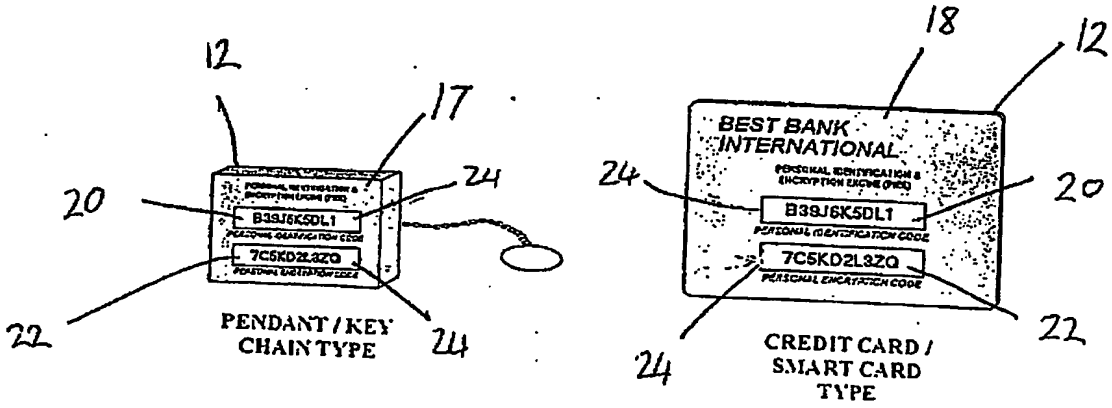

12
17
20
24
B39J6K5DL1
7C5KD2L3ZQ
22
24
PENDANT / KEY CHAIN TYPE
18
12
BEST BANK INTERNATIONAL
24
20
B39J6K5DL1
7C5KD2L3ZQ
22
24
CREDIT CARD / SMART CARD TYPE

Fig 1

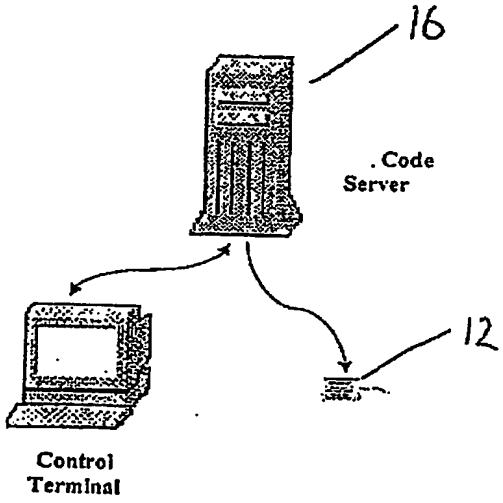

16
Code Server
12
Control Terminal

Fig 2

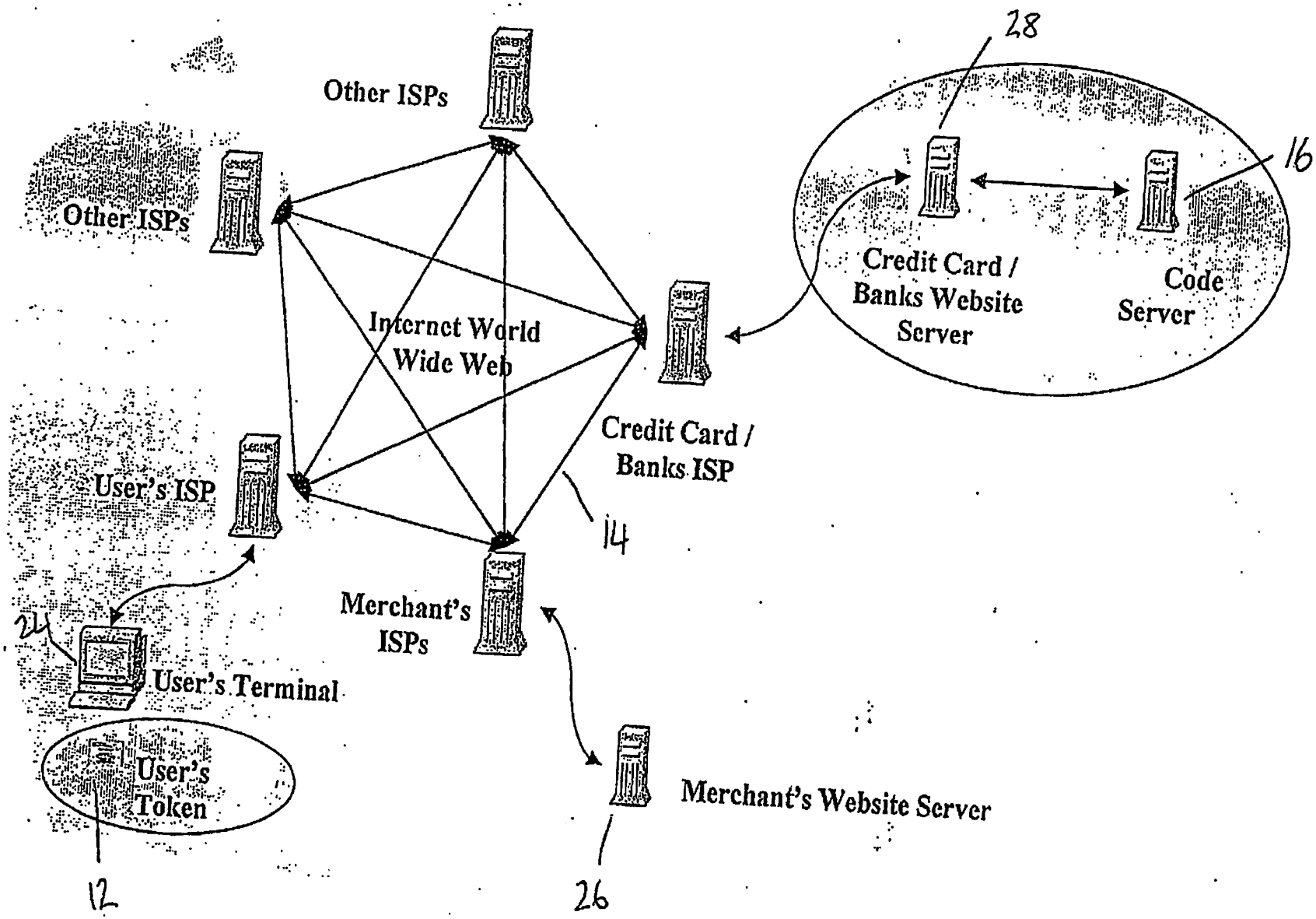

Other ISPs
Other ISPs
Internet World Wide Web
User's ISP
Credit Card / Banks ISP
14
Merchant's ISPs
24
User's Terminal
User's Token
12
Merchant's Website Server
26
28
Credit Card / Banks Website Server
Code Server
16

Fig 3

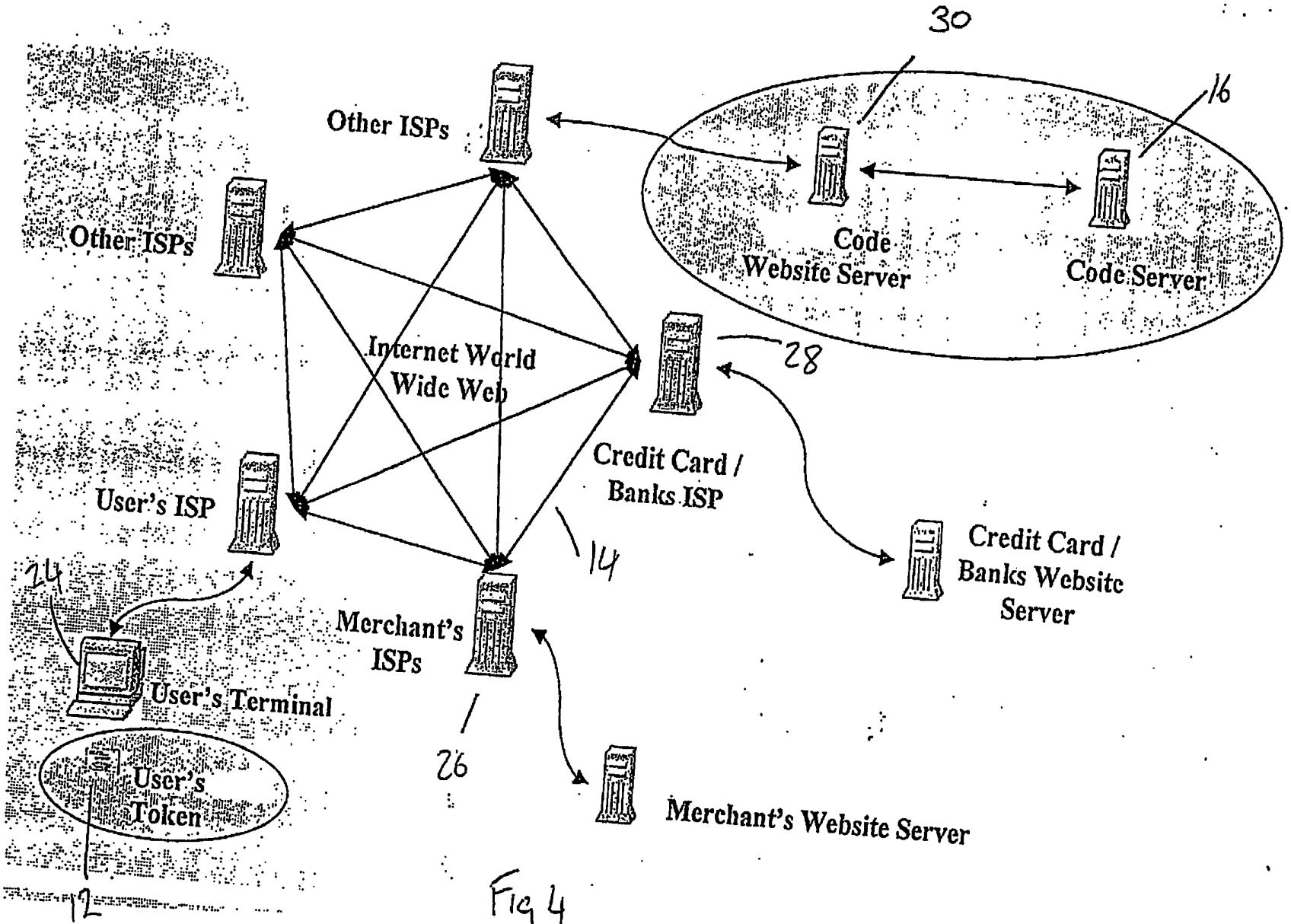
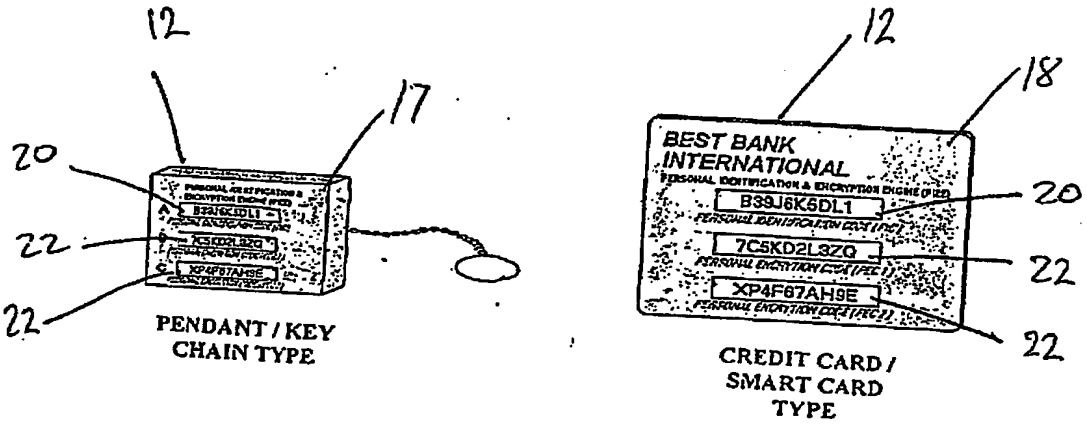

30
16
Other ISPs
Other ISPs
Code
Website Server
Code Server
Internet World
Wide Web
28
Credit Card /
Banks ISP
User's ISP
14
Credit Card /
Banks Website
Server
24
Merchant's
ISPs
User's Terminal
User's
Token
26
Merchant's Website Server
12

Fig 4



PENDANT / KEY CHAIN TYPE

CREDIT CARD / SMART CARD TYPE

Fig 5